УДК 343.985.2:343.140.02

Д. В. Яковчик,
курсант 3-го курса факультета милиции
Могилевского института МВД
Научный руководитель: М. Н. Манько,
старший преподаватель кафедры
уголовного процесса и криминалистики
Могилевского института МВД

ШЕРЛОК В «ЦИФРАХ»: ТАКТИКА СБОРА И ПРОБЛЕМА ИСПОЛЬЗОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В УГОЛОВНОМ ПРОЦЕССЕ

Анализ совершаемых преступлений в Республике Беларусь за последние годы показывает значительный рост количества преступлений, совершаемых в сфере высоких технологий. В первую очередь это объясняется развитием средств в данной сфере, увеличением роли компьютерных технологий в жизни человека, а также стремительным прогрессом человеческих возможностей в их использовании.

Не отстают от развития преступности в сфере высоких технологий и меры, принимаемые для противодействия совершению таких преступлений. Одним из методов раскрытия преступлений в данной сфере является сбор компьютерной информации.

Информация занимает центральное место в познавательной деятельности сотрудников органов уголовного преследования, поэтому поиск путей более быстрого и полного получения информации является важным направлением в криминалистике [1, с. 138]. При этом очевидной проблемой является отсутствие правовой регламентации порядка получения компьютерной информации. Не указана в уголовно-процессуальном законодательстве и сама позиция относительно компьютерной информации как источника доказательств.

Сбор информации, если говорить в общем, производится с жестких дисков, оперативной памяти, трафика. Причем при определенных условиях любой электронный элемент может стать непосредственным носителем компьютерной информации: электронные документы, файлы, видео, фото. При сборе данных любая информация, сформированная программными средствами, может представлять интерес. Процесс сбора и фиксации информации обуславливается теми виртуальными следами, которые могут помочь при сборе (например, выполнение операций с содержимым памяти компьютера отображается в журнале администрирования, сведения о работе в сети Интернет — в log-файлах).

Сам сбор виртуальных следов представляет собой копирование, изъятие, сохранение либо скачивание этих следов. При этом указанные действия рекомендуется проводить совместно с лицами, обладающими специальными знаниями в сфере высоких технологий, так как велик риск утраты, изменения данных, внесения посторонних данных, что в дальнейшем может привести к невозможности их применения в уголовном процессе.

Наиболее распространенный способ фиксации подобной информации — закрепление в протоколе следственного действия (например, в протоколе осмотра компьютерной информации) с указанием устройства, в котором обнаружены виртуальные следы, собственника устройства, наличия подключения к глобальной сети Интернет, операционной системы, наименования обследуемого файла, даты и времени его создания и изменений. Помимо этого, рекомендуется использование фото- и видеосъемки для физической фиксации, резервное копирование файлов на собственные носители или архивы (облака), создание копий, а также производство распечатки результатов работы программных модулей.

Таким образом, компьютерная информация может выступать в качестве источников доказательств, полученных в порядке, предусмотренном уголовно-процессуальным законом. Методами ее сбора являются копирование, изъятие, скачивание виртуальных следов преступления и другие методы. Фиксация подобной информации заключается в закреплении сведений об этой информации в протоколе следственного действия, а также в принятии мер для сохранения виртуальных следов, например, создание ее копий или сохранение на несколько источников. Уголовно-процессуальный кодекс (далее — УПК) не дает определение термину «электронный носитель доказательств», однако по общепринятым представлениям под таким носителем понимается материальный носитель, используемый для записи, хранения и воспроизведения данных, обрабатываемых с помощью средств вычислительной техники [2]. Решение проблемы использования данных следов в уголовном процессе как источника доказательств видится в изменении уголовно-процессуального законодательства [3], а именно в уточнении ч. 1 ст. 88 УПК с указанием, что доказательствами могут быть сведения в виде компьютерной информации, и дополнении ч. 2 ст. 100 УПК указав, что к другим носителям информации относятся также иные носители информации, в том числе электронные, полученные, истребованные или представленные в порядке, предусмотренном УПК.

1. Гамбарова Е. А. К вопросу об использовании информации из социальных сетей в работе следователя // Вектор науки ТГУ. Сер., Юрид. науки. 2017. № 1 (28). С. 137–141. Вернуться к статье

2. Манько М. Н., Родько К. В. К вопросу о получении и проверке информации, хранящейся на электронных носителях, как источнике доказательств при расследовании уголовных дел [Электронный ресурс] // Актуальные проблемы науки и практики : сб. науч. тр. / Дальневост. юрид. ин-т МВД России. Хабаровск, 2020. Вып. 6. С. 432–435. URL: http://двюи.мвд.рф/Institut/Struktura/OTDELI/Redakcionno_izdatelskij_otdel/электронные-издания (дата обращения: 28.05.2022). Перейти к источнику Вернуться к статье

3. Савчук Т. А. Цифровые доказательства как элемент информационной модели уголовного процесса // Совершенствование следственной деятельности в условиях информатизации : сб. материалов междунар. науч-практ. конф., Минск, 12–13 апр. 2018 г. / Промышленно-торговое право. Минск, 2019. Вернуться к статье